Co-funded by the
Erasmus+ Programme
of the European Union

A KNOWLEDGE ALLIANCE FOR BLOCKCHAIN IN ACADEMIC, ENTREPRENEURIAL AND INVESTMENT TRAINING

601063-EPP-1-2018-1-CY-EPPKA2-KA

Translated Syllabi-Italian

Deliverable 15
WP5: Content Development Task 5.3

September 2020

DLT4All Curriculum

Italian translation

Co-funded by the
Erasmus+ Programme
of the European Union

Sommario

Autori

Name	Partner
Claudio Schifanella	UNITO
Fadi Barbara	UNITO
Elisabetta Giromini	ComoNExT

Co-funded by the
Erasmus+ Programme
of the European Union

Introduzione

Questo documento presenta i risultati delle attività svolte dal partenariato nell'ambito dell'attività T3.9, incentrate sull'analisi, il consolidamento e l'elaborazione dei risultati prodotti da tutti i partner durante lo studio precedente delle diverse otto priorità di formazione tematiche (attività da T3.1 a T3.8). In questa fase preliminare, tutti i temi focali per la formazione sono stati approfonditi, sia attraverso l'attività di esperti del settore, sia da una serie di otto laboratori di co-design di un giorno ciascuno, che si sono svolti in 5 diversi paesi e hanno coinvolto più di 150 partecipanti. I risultati di queste attività sono stati raccolti e presentati nel precedente deliverable D9 “Moduli di formazione”.

Questo documento presenta il risultato del processo di co-design del Curriculum di DLT4All. Tutte le proposte contenute negli otto precedenti report sono state analizzate, ulteriormente elaborate e rese coerenti tra loro, al fine di creare un percorso di formazione in grado di garantire agli utenti target di DLT4All (studenti, investitori, imprenditori e gestori di incubatori) di acquisire le competenze e il know-how rilevanti sulle tecnologie DLT, sia dal punto di vista tecnico che di business. Le sezioni seguenti contengono, per ogni Modulo di formazione, una descrizione, l'elenco degli obiettivi di formazione attesi e un programma dettagliato di argomenti che saranno utilizzati come input nella Metodologia di implementazione DLT4All (WP4), così come nel Content Development (WP5).

Nonostante la proposta iniziale, l'analisi del materiale prodotto da ciascun partner durante lo sviluppo dei moduli di formazione ha evidenziato la necessità di offrire al pubblico un modulo formativo iniziale che fornisca un'introduzione al corso DLT4All e alle tecnologie DLT: questo fornirà agli utenti un quadro generale dell'intero curriculum, aumentando la consapevolezza e il coinvolgimento.

In sintesi, il curriculum che il progetto DLT4All propone è costituito dai seguenti Moduli Formativi (Learning Modules, LM):

- **LM0** – Introduzione al corso e al mondo delle DLT
- **LM1** – Design dei Database Peer-to-peer
- **LM2** – Tecniche di crittografia
- **LM3** – Meccanismi di consenso
- **LM4** – Firme digitali
- **LM5** – Smart Contracts
- **LM6** – Privacy e diritti di proprietà
- **LM7** – Applicazioni decentralizzate basate su blockchain (dApps)
- **LM8** – Organizzazioni autonome decentralizzate (DAOs)

Co-funded by the
Erasmus+ Programme
of the European Union

Modulo di formazione 0: Introduzione al corso e al mondo DLT4All

Il Modulo di formazione 0 è diviso in due parti.
La prima parte fornisce un'introduzione al corso DLT4All, identificando i diversi destinatari e le parti del curriculum che sono rivolte a ciascuno di loro e presentando una panoramica delle opzioni di certificazione disponibili.
La seconda parte offre un'introduzione alle tecnologie Blockchain sia da una prospettiva storica che da un punto di vista tecnico. Viene presentata una panoramica della struttura di una Blockchain e vengono introdotti i concetti fondamentali, che saranno sviluppati nei seguenti moduli del corso. Viene fornita una tassonomia di Blockchain basata sui permessi di lettura e scrittura e vengono introdotti i concetti di criptovaluta, smart contract e applicazione decentralizzata. Una panoramica dei casi d'uso della blockchain conclude il Modulo di formazione.

Obiettivi formativi

- Presentare la struttura e il contenuto del corso DLT4All
- Definire i diversi destinatari del corso DLT4All
- Descrivere le opzioni di certificazione disponibili per i partecipanti
- Fornire una panoramica storica dello sviluppo della tecnologia Blockchain
- Fornire una panoramica delle componenti tecnologiche di un sistema basato su blockchain
- Presentare una caratterizzazione delle Blockchain basata sui permessi di lettura / scrittura dell'utente
- Descrivere i concetti di criptovaluta, Smart Contract e applicazione decentralizzata nel contesto di un sistema basato su blockchain
- Presentare una serie di casi d'uso rilevanti in sistemi basati su blockchain

Risultati attesi

- Conoscenza della struttura del corso DLT4All
- Scelta rispetto a quale target group della formazione appartenere
- Comprensione delle opzioni di certificazione disponibili
- Conoscenza dello sviluppo storico delle tecnologie blockchain
- Conoscenza delle componenti tecniche di un sistema basato su blockchain
- Conoscenza della classificazione delle blockchain
- Conoscenza dei concetti di criptovaluta, contratto intelligente e applicazione decentralizzata
- Conoscenza applicative tramire i casi d'uso rilevanti in tema blockchain

Programma

1. Introduzione al corso DLT4ALL

    1.1. Destinatari

    1.2. Struttura del corso

    1.3. Opzioni di certificazione

2. Introduzione alla Blockchain

    2.1. Panoramica storica

    2.2. Componenti tecnologiche di un sistema basato su blockchain

3. Caratterizzazione delle Blockchain

    3.1. Pubblico vs privato e senza autorizzazione vs autorizzato

4. Dalle Blockchain alle dApp

    4.1. Criptovalute

    4.2. Contratti intelligenti

    4.3. Applicazioni decentralizzate

5. Casi d'uso

Co-funded by the
Erasmus+ Programme
of the European Union

Modulo di formazione 1: progettazione di database peer-to-peer

Descrizione

La possibilità di avere banche dati aperte e condivise con dati certificati e verificabili pubblicamente può portare al coinvolgimento e all'empowerment dei cittadini in molte aree.
Il Modulo di formazione 1 accompagna in una discussione approfondita sui problemi di progettazione architettonica della gestione dei dati. Le sfide affrontate nella progettazione di un database distribuito e decentralizzato vengono presentate e analizzate nel dettaglio, introducendo i principi di base della progettazione di database e i meccanismi alla base delle reti di comunicazione peer-to-peer. Vengono presentate le difficoltà incontrate nello sviluppo di un database peer-to-peer affidabile e le potenziali soluzioni a tali problemi fornite dalle tecnologie blockchain.
I partecipanti capiranno come un database può essere condiviso e sincronizzato tra diversi nodi e perché non è facile modificarne la struttura in seguito. Saranno così in grado di determinare quando è appropriato utilizzare un database distribuito. Capiranno perché un database distribuito è affidabile e come questa tecnologia può rendere più sicure le transazioni e la condivisione dei dati all'interno delle catene di approvvigionamento. Potranno riconoscere che in alcuni casi vale la pena creare una nuova blockchain ad-hoc, mentre in altri è meglio utilizzare una blockchain esistente per garantire l'integrità dei dati scambiati con i propri fornitori.

Prerequisiti

Il modulo non ha prerequisiti.

Obiettivi della formazione

- Spiegare cos'è un database e le basi di come funziona.
- Introdurre i concetti di base della tecnologia di comunicazione peer-to-peer (P2P) e i suoi vantaggi rispetto al paradigma tradizionale.
- Spiegare i metodi utilizzati per creare un database in un ambiente P2P (cioè la blockchain).
- Discutere criticità, limiti e svantaggi dell'utilizzo della tecnologia blockchain invece di un database centralizzato.
- Presentare casi d'uso in cui l'uso della tecnologia blockchain risulta vantaggioso.

Risultati attesi

- Comprendere le basi della progettazione di database.
- Comprendere i meccanismi di funzionamento di base delle reti di comunicazione peer-to-peer.
- Comprendere perché la tecnologia blockchain è stata sviluppata come soluzione ai problemi affrontati nella progettazione di un database distribuito peer-to-peer.
- Saper spiegare in quali casi i database peer-to-peer possono o non possono essere utili.
- Comprendere perché l'integrità dei dati non è una garanzia di accuratezza delle informazioni quando è coinvolto il fattore umano.

Programma

1. Cosa è un database e come funziona
    1.1. Principi del database, come funziona un database oggi
    1.2. Dove i database funzionano meglio e perché è necessaria una nuova tecnologia
2. Che cos'è il peer-to-peer e come si differenzia dal paradigma di comunicazione tradizionale

Co-funded by the
Erasmus+ Programme
of the European Union

Modulo di formazione 2: tecniche di crittografia

Descrizione

Le tecnologie blockchain si basano su un'ampia varietà di primitive crittografiche e tecniche per garantirne il funzionamento. I blocchi successivi in una blockchain in continua crescita sono collegati tra loro tramite funzioni hash crittografiche. Gli account su una blockchain sono identificati da chiavi pubbliche crittografiche e le chiavi private corrispondenti vengono utilizzate per autorizzare le transazioni. Le tecniche di crittografia sono un concetto fondamentale per la comprensione delle DLT in generale e delle blockchain in particolare.
Il Modulo di formazione 2 introduce e descrive in profondità i concetti di crittografia che sono centrali per questa tecnologia. I principi di base della crittografia e della crittoanalisi sono presentati in una panoramica iniziale. Viene introdotto il concetto di funzione hash e vengono forniti esempi di funzioni hash e relative applicazioni. Le tecniche di crittografia simmetrica e asimmetrica vengono discusse in dettaglio, con esempi e una sessione di laboratorio dedicata. Viene introdotto il concetto di Zero-Knowledge Proofs e discusse le applicazioni della crittografia nello spazio blockchain.

Prerequisiti

Questo modulo non ha prerequisiti

Obiettivi formativi

- Introdurre le caratteristiche chiave della crittografia e i suoi possibili usi in Blockchain.
- Presentare in modo comparativo differenti crittosistemi e la loro evoluzione.
- Descrivere il concetto di funzione hash e presentare comparativamente un insieme di funzioni hash utilizzate nei sistemi basati su blockchain.
- Spiegare i concetti fondamentali dei sistemi di crittografia simmetrici e asimmetrici.
- Presentare tecniche crittografiche a tutela della privacy e Zero-Knowledge Proofs.
- Illustrare come le tecniche crittografiche vengono applicate nei sistemi basati su blockchain.
- Presentare casi d'uso rilevanti costruiti attorno alla crittografia Blockchain.

Risultati attesi

- Comprendere i concetti chiave della crittografia.
- Esaminare quale sistema crittografico è più adeguato a seconda del caso d'uso previsto.
- Identificare e analizzare le diverse funzioni hash.
- Identificare e analizzare le applicazioni della crittografia simmetrica e asimmetrica.
- Discutere e analizzare metodi crittografici a tutela della privacy e Zero-Knowledge Proofs.
- Identificare e valutare le applicazioni dei metodi crittografici nei sistemi basati su blockchain.
- Esaminare come vengono utilizzate le tecniche di crittografia nei casi d'uso rilevanti della blockchain.

Programma

1. Introduzione alla crittografia
    - 1.1. Cos'è la crittografia?
    - 1.2. Classificazione dei criptosistemi
    - 1.3. Principi di base
    - 1.4. Principali criptosistemi classici ed evoluzione
    - 1.5. Perfette condizioni di crittografia
    - 1.6. Crittanalisi

2. Funzioni hash
    2.1. Cos'è una funzione hash?
    2.2. Tipi di funzioni hash: MD5, SHA-x
    2.3. Laboratorio: sperimentazione con funzioni hash
3. Crittografia simmetrica
    3.1. Definizione
    3.2. Crittografia Vernam, Flow e Block
4. Crittografia asimmetrica
    4.1. Definizione
    4.2. Algoritmi di scambio di chiavi (Diffie-Hellman)
    4.3. RSA
5. Laboratorio: sperimentazione con crittografia simmetrica e asimmetrica
6. Zero-Knowledge Proofs (Prove a conoscenza zero)
7. Applicazioni della crittografia Blockchain
    7.1. Applicazione negli scambi QR
    7.2. Gestione degli indirizzi Bitcoin ed Ethereum
    7.3. Pratica della teoria dei blocchi
8. Casi d'uso: settore finanziario, sanità, servizi legali, difesa, pubblica amministrazione, digitalizzazione industriale, progetti sociali, lotta alla povertà, gestione dell'identità individuale

Modulo di formazione 3: Meccanismi di consenso

Descrizione

Uno dei problemi centrali nella progettazione di un sistema blockchain è la scelta del meccanismo utilizzato dai nodi della rete per raggiungere il consenso sullo stato del sistema in maniera decentralizzata, cioè senza ricorrere a una parte centrale che agisca sulla fiducia.
Il Modulo di formazione 3 esplora i meccanismi attuali che gestiscono l'accordo tra tutti i nodi che partecipano a un sistema blockchain. Verranno discussi i meccanismi di consenso più utilizzati, con eguale enfasi sia sugli aspetti tecnici che commerciali dell'argomento.
All'inizio del modulo, viene presentata la necessità di un meccanismo di consenso in un ambiente di database distribuito e vengono discusse le soluzioni per i sistemi autorizzati. Viene presentato il ruolo della teoria dei giochi nella progettazione del meccanismo di consenso. Viene fornita una classificazione dei diversi meccanismi di consenso che sono stati implementati nella pratica o proposti in teoria all'interno delle due ampie categorie di meccanismi Proof of Work (PoW) e Proof of Stake (PoS) e vengono descritti i potenziali attacchi a tali meccanismi. Successivamente, viene presentata una mappatura dei diversi meccanismi al trade-off tra incentivi per mantenere la blockchain e sicurezza contro attacchi dannosi che possono compromettere l'integrità della blockchain, con particolare considerazione della posizione che ogni particolare meccanismo occupa nello spazio di centralizzazione-decentramento. La parte finale del modulo presenta una serie di casi di studio pratici.
I partecipanti che completano questo modulo saranno in grado di cogliere i vantaggi e gli svantaggi di qualsiasi protocollo di consenso nel contesto di qualsiasi modello di business specifico basato su un libro mastro distribuito (distributed ledger), nonché i suoi limiti in termini di precisione, efficienza dei costi, grado di decentralizzazione, scalabilità, velocità di elaborazione e sostenibilità della rete.

Prerequisiti

Questo modulo di formazione ha i seguenti prerequisiti:

- Progettazione di database P2P (LM1)
- Tecniche di crittografia (LM2)

Obiettivi formativi

- Spiegare la necessità di un meccanismo di consenso in un sistema basato su blockchain.
- Presentare i meccanismi di consenso utilizzati nelle configurazioni blockchain autorizzate.
- Discutere il ruolo della teoria dei giochi nella progettazione di un meccanismo di consenso.
- Presentare protocolli di consenso Proof-of-Concept (PoX) più ampiamente utilizzati nei sistemi blockchain.
- Discutere possibili attacchi ai protocolli di consenso distribuito.
- Introdurre e descrivere strutture di incentivi utilizzate nei protocolli di consenso distribuito.
- Presentare attacchi ai protocolli di consenso relativi alle strutture di incentivi.
- Discutere i costi dei protocolli di consenso distribuito comunemente usati.
- Discutere le proprietà di prestazioni e scalabilità dei protocolli di consenso distribuito ampiamente utilizzati.
- Presentare soluzioni ai problemi di scalabilità basate su alternative ai protocolli di consenso distribuito dove sono utilizzati sistemi basati su blockchain.
- Presentare casi d'uso di diversi meccanismi di consenso distribuito in diversi sistemi blockchain.

Risultati attesi

- Comprensione del ruolo del consenso nelle DLT e nei sistemi Blockchain.
- Comprensione del funzionamento dei protocolli di consenso distribuito di tipo PoX.

- Conoscenza dei possibili attacchi dei protocolli di consenso distribuito.
- Saper confrontare costi, prestazioni, scalabilità e sicurezza tra i protocolli di consenso analizzando le loro specifiche di progettazione.
- Saper valutare le caratteristiche desiderate di un protocollo di consenso per uno specifico modello di business.

Programma

1. Introduzione
    1.1. La necessità di meccanismi di consenso
    1.2. Blockchain autorizzate: consenso attraverso meccanismi di voto Byzantine-Fault Tolerant (BFT)
2. Il ruolo della teoria dei giochi nel consenso
3. Protocolli Proof-of-Concept (PoX)
    3.1. Il concetto di consenso probabilistico e sue proprietà
    3.2. Lotterie di puzzle crittografici e proprietà richieste
    3.3. Protocolli principali: Proof-of-Work, Proof-of-Stake, Proof-of-Stake delegato, Proof-of-Authority
    3.4. Una tassonomia dei potenziali attacchi: attacchi Sybil, attacchi di razza, attacchi di Finney, attacchi del 51%
4. Incentivi
    4.1. Teoria di base: costi irrecuperabili, problemi principale-agente e compatibilità degli incentivi
    4.2. Compatibilità degli incentivi nei protocolli PoX: token, mining pool e mining cartels
    4.3. Mercati in gettoni
    4.4. Vulnerabilità dei protocolli PoX: mining egoistico, block withholding, pool di mining in attesa, pool hopping
5. Costi
    5.1. La natura costosa dei protocolli PoX
    5.2. Protocolli Proof-of-Stake (PoS) e la tragedia del problema dei beni comuni
    5.3. Problemi di sicurezza nei protocolli PoS: attacchi Nothing-at-stake, attacchi grinding
6. Prestazioni
    6.1. Le prestazioni limitate delle blockchain senza autorizzazione
    6.2. Protocolli ibridi
    6.3. Interoperabilità blockchain
    6.4. Reti blockchain non lineari: protocollo Greedy Heaviest-Observed Sub-Tree (GHOST)
    6.5. Protocolli basati su Direct Acyclic Graph (DAG)
7. Esempi
    7.1. Tessuto Hyperledger (BFT)
    7.2. Bitcoin (PoW)
    7.3. Primecoin (PoUS)
    7.4. Filecoin (UPoW)
    7.5. SpaceMint (PoSP)
    7.6. Bytecent (PoH)
    7.7. Peercoin (PoS)
    7.8. Algorand (protocolli ibridi)
    7.9. Teechain su Bitcoin (reti a catena laterale)
    7.10. Implementazione di Ethereum Casper (GHOST)

Learning module 4: Digital Signatures

Description

Digital signatures are the extension of paper signatures to the digital realm that is made possible thanks to the development of asymmetric cryptography. Like real signatures, they are a way to prove one's identity and to certify the origin of a message.

Learning Module 4 describes the properties and technical requirements necessary for the implementation of digital signatures and the mathematical prerequisites. The generic characteristics of a digital signature algorithms are then presented and specific algorithms that are commonly used in blockchain systems implementation are discussed in detail. Privacy preserving digital signature algorithms are discussed, focusing on their use in the cryptocurrency space and concepts of anonymity and pseudonymity of transaction on a blockchain are presented. Security of digital signatures and possible attack schemes are considered and an in-depth analysis of one possible attack vector is analyzed in a lab. The last part of the module discusses the future of digital signatures, presenting novel algorithms designed to be resistant to present and foreseen threats linked to the advent of quantum computers.

Dependencies

This learning module has the following prerequisites:

- Encryption techniques (LM2)

Learning Objectives

- To explain basic properties that a digital signature algorithm must satisfy.
- To present the digital signature algorithms that are most widely used in blockchain-based systems
- To present privacy-preserving digital signature algorithms.
- To discuss anonymity and pseudonymity features of blockchain systems.
- To present attacks and security issues related to digital signature algorithms.
- To present beyond state-of-the-art development related to digital signature algorithms.
- To present use cases of digital signatures in blockchain-based systems.

Learning Outcomes

- **Understand** fundamental properties of digital signature algorithms.
- **Understand** details of the most used digital signature algorithms
- **Acquire** technical skills related to the use of digital signatures.
- **Understand** the workings of privacy preserving digital signature algorithms.
- **Recite** possible attacks on commonly used digital signature algorithms.

Syllabus

1. Signature definitions, properties, and requests
2. Preliminaries
   2.1. Elliptic Curves

2.2. Lab: the bitcoin-core/secp256k1 library

3. Digital signature algorithms
   3.1. Introduction
   3.2. DSA
   3.3. ECDSA
   3.4. Schnorr signatures
   3.5. Lab: implementation and analysis of Schnorr signatures
4. Ring signatures
   4.1. Properties
   4.2. The role of ring signatures in the Monero blockchain
   4.3. Lab: implementing ring signatures
5. Anonymity and pseudonymity in blockchain transactions
6. Security and Attacks
   6.1. Overview of security problems and attacks
   6.2. Lab: specific attack on Schnorr signatures
7. The Future of Digital Signatures: Lattices, hash signatures, and threshold signatures
8. Use cases

Learning module 5: Smart Contracts

Description

The term “Smart Contracts” is used with two separate interpretations:

- “A Smart Contract is a collection of code (its functions) and data (its state) that resides at a specific address on the blockchain.”
- “A Smart Contract (as a Contract) is a computer protocol intended to digitally facilitate, verify, or enforce the negotiation or performance of a contract.”

Learning Module 5 investigates design issues of blockchain-based applications (Smart Contracts) that can automatically execute the terms of a contract, focusing on both technological and business aspects of the subject.

The module begins with an introduction to the concept of Smart Contract and a description of its historical development. An overview of programming languages used for development of Smart Contracts for blockchain systems and execution environments is presented, followed by a detailed description of the Ethereum Virtual Machine and a thematic lab on development of Smart Contract for the Ethereum platform using the Solidity programming language. Oracles, a special category of Smart Contracts that communicate with trusted entities, are described in detail. Computational costs and security issues of Smart Contract programming are discussed, and best practices adopted to mitigate problems and risks presented. Finally, the Smart Contracts could be used as a contract, the main regulatory and legal issues about the Smart Contracts should are identified and described.

Dependencies

This learning module has the following prerequisites:

- Consensus mechanisms (LM3)
- Digital Signatures (LM4)

Learning Objectives

- To define and explain basic properties of a Smart Contract.
- To present different programming languages used to develop Smart Contracts and their execution environments.
- To describe the Ethereum blockchain and the Ethereum Virtual Machine.
- To explain how to use the Solidity language to develop a Smart Contract for the Ethereum Blockchain.
- To present the concept of Oracles their basic functioning principles.
- To discuss the computational costs of deploying and executing a Smart Contract and the role of Gas on the Ethereum Blockchain.
- To discuss security issues related to the development and use of Smart Contracts.
- To present regulation frameworks affecting the use of Smart Contracts.
- To present legal issues related to the use of Smart Contracts in a blockchain-based system.

Learning Outcomes

- **Describe** the basic concepts of Smart Contracts.

- **Recognize** different Smart Contracts' programming languages and their execution environments.
- **Identify** the key features of different Smart Contracts' programming languages.
- **Describe** the Ethereum Blockchain.
- **Explain** how the Ethereum Virtual Machine works.
- **Implement** Smart Contracts in Ethereum using Solidity.
- **Examine** the computational cost of deploying and using a Smart Contract in Ethereum.
- **Demonstrate** Smart Contracts' use cases in multiple domains.
- **Understand** current technology's restrictions and limitations.
- **Identify** issues related to the development of Smart Contracts.
- **Examine** advantages and disadvantages of using a Smart Contract.
- **Identify** concerns about security, stability and cost of a Smart Contract.
- **Assess** whether a Smart Contract solution is suitable for the problem under study.
- **Assess** how and when to apply Smart Contracts in real-life applications.
- **Implement** Smart Contracts in real-life applications.

Syllabus

1. Smart Contracts
   1.1. History, Definition, Simple use cases
   1.2. Introduction to "Smart Contracts" in Blockchain
   1.3. The lifecycle of a Smart Contract (theory)
2. Smart Contracts' Languages
   2.1. Reference to the different Blockchain environments and account of their key features: Ethereum, Hyperledger Fabric.
   2.2. Evolution of Blockchain Scripting Languages
   2.3. Overview of the key features of different high-level programming languages for various Blockchain environments
   2.4. Introduction to Smart Contract's Execution Environments
   2.5. Analysis of Ethereum Virtual Machine - EVM: Main Characteristics, Programming languages, Restrictions
3. Lab: Development in Ethereum with Solidity language
   3.1. Basic Data Types & Statements, Specific Data Types, Data Structures, Access Modifiers & Applications.
   3.2. Design Techniques
   3.3. A Smart Contract's lifecycle in practice: compilation, deployment, interaction and destruction
4. Oracles
   4.1. Introduction to oracles
   4.2. Develop contracts that will communicate with trusted entities in the real world
5. Computational Cost
   5.1. The role of gas in Ethereum
   5.2. Analysis of the cost of transactions
   5.3. Analysis of the cost of a Smart Contract
6. Security
   6.1. Issues: known 'hacks' and problems.

6.2. Solutions: security libraries, open known standards, best practices, analysis tools.
6.3. Key problems and Solutions strategies

7. Regulation Frameworks
   7.1. Overview of existing regulations for Smart Contracts
   7.2. Analysis of the laws that concern Smart Contracts

8. Legal Issues
   8.1. Clarify the Legal issues regarding Smart Contracts
   8.2. Political and environmental aspects

Learning module 6: Privacy and Property Rights

Description

Computing is no longer operating in a vacuum and as such it affects and is affected by society. Moreover, in most cases technology is ahead of society settings and legislation, and, in most cases both society and legislation need to catch up and adapt to the new situation as defined by the technology. In rare occasions, however, the technology is coming to the aid of legislation and society, and, allows certain operations to take place in a more transparent and faster fashion than current practices allow.

Learning Module 6 discusses how blockchain technology can support legislation on Property Rights, both tangible and intangible and describes privacy related issues in blockchain. The European legislation on property rights and licensing is presented and how blockchain technologies could help designing a fair remuneration scheme is discussed. The GDPR and issues related to privacy are then discussed, together with implication related to blockchain immutability for rights that need to be guaranteed under GDPR (like the right to be forgotten). Finally, technologies to enhance privacy of blockchain-based systems are presented and related issues discussed in detail.

Dependencies

This learning module has the following prerequisites:

- Introduction to the DLT world (LM0)
- Smart Contracts (LM5)

Learning Objectives

- To present the current European legislation framework related to Property Rights.
- To describe existing types of software licenses.
- To explain international copyright laws.
- To discuss license coordination and the role of registries.
- To discuss issues related to Property Rights that arise when using DLTs.
- To present the European GDPR and its implications for privacy and information freedom.
- To discuss issues related to GDPR that arise when using DLTs.
- To present a set of privacy-preserving encryption techniques.
- To discuss issues related to privacy that arise in a DLT-based system.

Learning Outcomes

- **Understand** the GDPR and its implications for blockchain technologies.
- **Understand** how to avoid conflicts with the law when utilizing blockchain technology.
- **Describe** property rights can be protected utilizing blockchain.
- **Understand** how personal data can be in the control of individuals thanks to blockchain technology.
- **Describe** how Angel Investors can valuate Blockchain-related companies.
- **Recite** the role of IPR rights in encouraging innovation and creativity and how blockchain can accommodate/facilitate IPR.
- **Understand** how the property rights can be protected utilizing blockchain technology.
- **Examine** security and privacy considerations of storage integration.

Co-funded by the
Erasmus+ Programme
of the European Union

1. Property Rights
   1.1. The legislation around Intellectual Property Rights (CPDA 1988)
   1.2. What a software license is
   1.3. License types
   1.4. International copyright law
   1.5. Token as a license?
   1.6. Private ordering
   1.7. Fragmentation
   1.8. Licensing coordination
   1.9. Registries
   1.10. Formalities
   1.11. Orphan works and the public domain
   1.12. Rights management information
   1.13. Fair remuneration
2. DLT Issues pertaining to Property Rights
3. GDPR – Issues with privacy and Information Freedom
4. DLT Issues pertaining to GDPR
5. Applied encryption techniques for privacy
   5.1. Chameleon hash functions
   5.2. Stealth addresses
   5.3. Confidential transactions through ring signatures
   5.4. Implementing privacy through zero-knowledge proof
   5.5. Private smart contracts – Enigma
   5.6. Off-chain storage
6. Privacy issues of DLTs

Learning module 7: Blockchain-based Decentralized Applications

Description

Decentralized applications differ from centralized alternatives, as they enhance a peer-to-peer network of participants. The need for transacting parties to communicate without the essentiality of a central authority is a common topic of discussion and evaluation among technology enthusiasts. Such Decentralized Applications (dApps) can disrupt various industries, which were presented to the audience as use-cases *e.g.* examples in finance, academia, supply chain, energy sector and others.

Learning Module 7 analyses dApps in all their aspects and is addressed to both technical and non-technical audiences, always keeping the topic challenging. The main aim of the module is to enable participants to evaluate which industries are ready to adopt Blockchain technology and to which extent. Decentralization and disintermediation are novel concepts and difficult to fully grasp. There are plenty of components that need to be taken into consideration such as the degree of security, privacy and interoperability. Each DLT network varies to the extent of satisfying these components. It is of ultimate importance for the content creators to evaluate the best practices and potential shortcomings of this technology. The basic structure and main design patterns of dApps are presented as an introduction to the basics of dApps development. Use cases for advanced dApps in various sectors a presented together with their relation to other disruptive technologies within the framework of the 4th Industrial revolution.

Dependencies

This learning module has the following prerequisites:

- Introduction to the DLT world (LM0)
- Smart Contracts (LM5)

Learning Objectives

- To comparatively present the conditions under which traditional centralized models and dApps can be used.
- To associate the key characteristics of dApps with the fundamental properties of blockchains.
- To explain the meaning of functional and non-functional requirements within the context of dApps.
- To comparatively present different blockchains as candidates for dApps development.
- To illustrate how the information flows at the architectural level of dApps.
- To present the technological stack of dApps.
- To present a number of indicative use cases built around dApps.
- To explain the possible synergies of dApps with other emerging technologies.
- To discuss the possible legal implications of dApps.

Learning Outcomes

- **Assess** whether a dApp is required as opposed to the traditional centralized model.
- **Analyze** the key characteristics of dApps with the fundamental properties of blockchains.
- **Identify** and **analyze** the functional and non-functional requirements of dApps.
- **Assess** the suitability of different blockchains for dApps.
- **Design** information flow architectures for dApps.

- **Identify** and analyze the main technological layers of dApps.
- **Examine** how dApps are being utilized in specific use cases.
- **Relate** dApps with other emerging technologies.
- **Identify** any requirements that may raise legal issues.

Syllabus

1. High-level anatomy of dApp
   1.1. Overview of the blockchain application stack
   1.2. Backend examples
   1.3. Frontend examples
2. dApp design patterns
   2.1. Patterns on Interacting with the External World
   2.2. Data Management Patterns
   2.3. Security Patterns
   2.4. Contract Structural Patterns
3. Basic dApps development
   3.1. Programming of public blockchains
   3.2. Programming of private/permissioned blockchains
   3.3. dApps lifecycle
4. Use cases of advanced dApps
   4.1. Decentralized exchange markets
   4.2. Decentralized data markets
   4.3. Blockchain-verifiable certificates and self-sovereign identities
   4.4. Emerging topics in the broader framework of dApps
5. Moving from dApps to the 4th industrial revolution
   5.1. The relation between IoT, AI and blockchain technologies

Learning module 8: Decentralized Autonomous Organizations

Description

The Decentralized Autonomous Organizations (DAOs) are organizations that run autonomously and could make decentralized decisions through the use of technology, e.g. Blockchain Technology, Directed Acyclic Graphs (DAG) technology, the Hashgraph algorithm, etc. A Decentralized Autonomous Organization (DAO) is typically an organization that is run through protocols encoded as various types of computer programs called smart contracts.

DAOs are sometimes also referred to as Decentralized Autonomous Corporations (DAC). Their financial transactions and program protocol records are maintained on blockchain or similar technologies. These types of organizations are similar to any organization in real world, however in digital world the rules of an organization (e.g. a company) are not enforced digitally. They are digital and already there by nature. DAOs are like a cryptographic democracy for an organization, where every stakeholder is able to vote to add new protocols, change existing protocols, or include and exclude a member among other such types of rights.

Learning Module 8 discusses the main characteristics of DAOs, as well as, their pros and cons. Particular attention will be given to the legal, cultural and political implications of the use of this disruptive paradigm. One case study of a DAO is analyzed in detail. Finally, a lab specifically designed for technical audience, will explain how to implement DAOs in the Ethereum infrastructure.

Dependencies

The learning module has the following prerequisites:

- Introduction to the DLT world (LM0)
- Smart Contracts (LM5)
- Privacy and Property Rights (LM6)

Learning Objectives

- To introduce the concept of Decentralized Autonomous Organization (DAO) as an extension of a dApp.
- To present the structure and governance mechanisms within a DAO.
- To discuss advantages and disadvantages of using a DAO to manage an organization.
- To present security issues, legal liability issues and risks of DAOs.
- To discuss cultural and political implications of DAOs.
- To analyze in-depth a specific use case of DAO.
- To present possible future developments of DAOs.
- To demonstrate how to implement a DAO on the Ethereum blockchain using Solidity.

Learning Outcomes

- **Understand** the basic concept of DAO.
- **Understand** the advantages and disadvantages of using DAOs.
- **Recite** legal and security risks of DAOs.
- **Describe** most important case studies using DAOs.

- **Implement** a DAO in Solidity.

Syllabus

1. Introduction to Decentralized Autonomous Organizations (DAOs)
   1.1. Defining the DAOs
   1.2. From dApps to DAOs
   1.3. Structure of DAOs
   1.4. Democracy within DAOs
2. Advantages and Disadvantages
   2.1. Advantages of DAOs
   2.2. Disadvantages of DAOs
   2.3. Challenges with DAOs
   2.4. Effectiveness of DAOs
3. Security, Legal Liability, and Risks
   3.1. Security of DAOs
   3.2. Legal liability of DAOs
   3.3. Risks related to DAOs
4. Cultural and Political Implications
   4.1. Cultural differences and implications of DAOs
   4.2. Political systems and implementations of DAOs
5. A Case Study of Decentralized Autonomous Organizations (DAOs)
   5.1. Exploring a case of DAO
   5.2. Lessons learned from the case study
6. Future of DAOs
7. Lab: Implementing a DAO in Solidity